CLAIMS

What is claimed is:

1. A keypad security circuit comprising:

a comparitor adapted to perform a bit wise comparison of an driver signal and a resulting signal;

a column output driver coupled to said comparitor, said column output driver coupled adapted to drive a keypad strong driver signal on a column;

a row output driver coupled to said comparitor, said row output driver adapted to drive an keypad strong driver signal on a row;

a programmable column word constructor coupled to said row output driver, said programmable column word constructor adapted to provide a weak driver signal on a column; and

a programmable row word constructor coupled to said column output driver, said programmable row word constructor adapted to provide a weak driver signal on said row.

2. The keypad security circuit of claim 1 wherein a set of digital values randomly varies over both the bits in each digital word and overtime.

3. The keypad security circuit of claim 2 wherein a set of random digital values is from a register file and are sequentially sent to the columns and rows as said column strong driver signal and said row strong driver signal.

3. The keypad security circuit of claim 2 wherein said column strong driver signal and said row strong driver signal both connect to the same bits from said register file.

4. The keypad security circuit of claim 2 wherein said register file is updated at random times or by significant events such as keypresses.

5. The keypad security circuit of claim 2 wherein said weak driver signals are changed to be independently pulled up or pulled down to support random bit values on each of said rows and columns.

6. The keypad security circuit of claim 2 wherein said column strong driver signal is a logical zero value when an opposing row weak driver signal is a logical one value.

7. The keypad security circuit of claim 2 wherein a row strong driver signal is a logical one value when an opposing column weak driver signal is a logical zero value.

8. The keypad security circuit of claim 2 wherein said programmable column word constructor and said programmable column word constructor comprise both a pull-up and a pull-down that are independently enabled.

9. A keypad security system comprising:

a keypad matrix comprising keys and corresponding switches that provide paths for conducting electricity between selected columns and rows of a switch matrix in response to activation of the switches resulting from manipulation of the keys;

a keypad security circuit coupled to said keypad matrix, said keypad security circuit adapted to provide security measures to safeguard switching sequences of said keypad matrix; and

a keypad scanner circuit coupled to said keypad security circuit, said keypad scanner circuit adapted to detect when a scan of signals from said keypad matrix indicates the status of a switch included keypad 230 changes.

10. A keypad security system of Claim 9 wherein said keypad scanner circuit is a standard keypad scanner circuit and said keypad matrix is a standard keypad matrix.

11. A keypad security system of Claim 10 wherein said keypad scanner circuit provides security measures to safeguard switching sequences by

utilizing a set of digital values that randomly varies over both time and the bits in each digital word input to a keypad row and column.

12. A keypad security system of Claim 10 wherein said set of random digital values are stored in a register file and are sequentially sent to said columns and rows of said keypad matrix.

13. A keypad security system of Claim 10 wherein the columns and rows both connect to the same bits from the register file.

14. A keypad security system of Claim 10 wherein said keypad scanner comprises

a keypad register adapted to provide the interface to a host processor;

a keypad interface ports coupled to said keypad register, said keypad ports adapted to provide communication paths for output and input signals;

a keypad state machine coupled to said keypad interface, controls the direction of keypad interface ports with the row and column output enable signals; and

a keypad debounce coupled to said keypad register, said keypad debounce adapted to provide a method of settling out the transitions of the switches between open and closed.

15 A keypad security method comprising the steps of :

driving a varying strong driver signal onto a first attribute of a keypad switch matrix;

applying a varying weak driver signal to a second attribute of a keypad switch matrix;

retrieving a resulting signal from said second attribute of the keypad switch matrix; and

forwarding a scanner input signal indicating the activation status of a switch on said second attribute.

16 A keypad security method of Claim 15 further comprising the steps of :

driving a varying strong driver signal to said second attribute of a keypad switch matrix;

applying a varying weak driver signal to said first attribute of a keypad switch matrix;

retrieving a resulting signal from said first attribute of the keypad switch matrix; and

forwarding a scanner input signal indicating the activation status of a switch on said first attribute.

17 The keypad security method of claim 15 wherein said first attribute of a keypad switch matrix is a column and said second attribute of a keypad switch matrix is a row.

18 The keypad security method of Claim 15 wherein said varying driver signal is one of a set of digital values that varies over both time and the bits in a digital keypad driver word.

19 The keypad security method of Claim 15 wherein said varying strong driver signal is generated by a randomizer and loaded into a register file.

20 The keypad security method of Claim 15 further comprising the step of utilizing a pull-up and a pull-down to provide with said weak driver signal to a second attribute of a keypad switch matrix, said pull-up and said-pull down are independently enabled.

21 The keypad security method of Claim 15 further comprising the step of performing keypress detection by binary comparison of said varying driver strong signal logical value on said first attribute of said keypad switch matrix and said resulting keypad signal logical value on said second attribute of said keypad switch matrix.

22 The keypad security method of Claim 15 further comprising the step of precharging said varying weak driver signal.

23 The keypad security method of Claim 15 further comprising the step of precharging said varying weak driver signal twice in one keypad clock cycle,

wherein said varying weak driver signal is precharged to a first logical value during a one portion of said keypad clock cycle and said varying weak driver signal is precharged to a second logical value during another portion of said keypad clock cycle.

24 The keypad security method of Claim 15 further comprising the step of sampling said resulting keypad signal twice during said keypad clock cycle.

25 The keypad security method of Claim 15 further comprising the step of debouncing said resulting keypad signal.